

# Configura alta disponibilità CMX

## Sommario

---

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Architettura](#)

[Infrastruttura di rete](#)

[IP virtuale](#)

[Passaggio 1. Installazione dell'interfaccia Web](#)

[Passaggio 2. Abilitare HA](#)

[Passaggio 3. Aggiungi Cisco WLC a CMX](#)

[Passaggio 4. Failover](#)

[Passaggio 5. Failback](#)

[Passaggio 6. Aggiorna/Disabilita HA](#)

[Come ricaricare in modo sicuro una coppia CMX HA](#)

[Verifica](#)

[Risoluzione dei problemi](#)

---

## Introduzione

Questo documento descrive i concetti fondamentali di Cisco Connected Mobile Experience (CMX) e come configurarlo.

## Prerequisiti

In questo documento viene descritto come abilitare l'alta disponibilità, aggiungere il controller WLC (Wireless LAN Controller) ed eseguire alcuni test che consentono di verificare la configurazione dell'alta disponibilità (HA, High Availability) con il failover/failback.

## Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- CMX
- Cisco WLC



Nota: HA non ha requisiti univoci per i controller LAN wireless.

---

## Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- CMX 10.6
- WLC 8,3

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

## Architettura

La componente centrale di un sistema ad alta disponibilità è il monitoraggio dello stato. Consente di configurare, gestire e monitorare l'impostazione HA. La modalità principale per mantenere la veglia è attraverso heartbeat tra primario e secondario. Il monitoraggio dello stato è responsabile dell'impostazione dei database (DB) e della replica dei file e, a sua volta, del monitoraggio dell'applicazione. CMX sotto il paradigma HA può essere definito come Primario o Secondario. La comunicazione con il mondo esterno (chiamate NMSP (Network Mobility Services Protocol) e API da endpoint di terze parti e Prime Infrastructure (PI)) avviene tramite un indirizzo IP virtuale. In questo modo, quando il server primario si guasta e il server secondario prende il controllo, l'IP virtuale viene commutato in modo trasparente.

La progettazione prevede un'interfaccia utente (UI) per la configurazione e il monitoraggio delle coppie HA. Gli allarmi vengono generati per CMX e all'esterno di CMX.

I database sono considerati il nucleo del sistema che deve essere sempre replicato in tempo reale senza perdita di dati. I dati dell'applicazione che si trovano all'esterno del database sono critici, ma non devono essere sincronizzati in tempo reale e non comportano una perdita di funzionalità.

## Infrastruttura di rete

Il sistema primario e quello secondario devono essere raggiungibili tra ogni sistema. Sia il database primario che quello secondario devono trovarsi nella stessa subnet. Questa operazione è necessaria in modo che l'indirizzo IP virtuale utilizzato possa essere commutato in entrambi i sistemi. Qualsiasi entità, ad esempio i controller LAN wireless, raggiungibile dal server primario deve essere raggiungibile anche dal server secondario. Affinché la sincronizzazione e il failover secondari funzionino correttamente, l'infrastruttura di rete deve consentire il flusso del traffico tra la porta primaria e quella secondaria. CMX utilizza il protocollo VRRP per verificare la presenza di keepalive da entrambe le unità CMX in Alta disponibilità, garantendo l'assenza di restrizioni tra le due unità in Alta disponibilità, in quanto il gateway deve essere raggiungibile per stabilire la raggiungibilità CMX.

Le porte verranno aperte su CMX, ma i firewall su CMX consentiranno solo agli altri sistemi peer di inviare il traffico su queste porte.

Porte	Descrizione
6378, 6379, 6380, 6381, 6382, 6383, 6385, 16378, 16379, 16380, 16381, 16382, 16383, 16385	Redis
7000, 7001, 9042	database Cassandra
5432	database Postgres
4242	Servizio Web e REST ad alta disponibilità
22	Porta SSH e utilizzata per sincronizzare i file tra i server

## IP virtuale

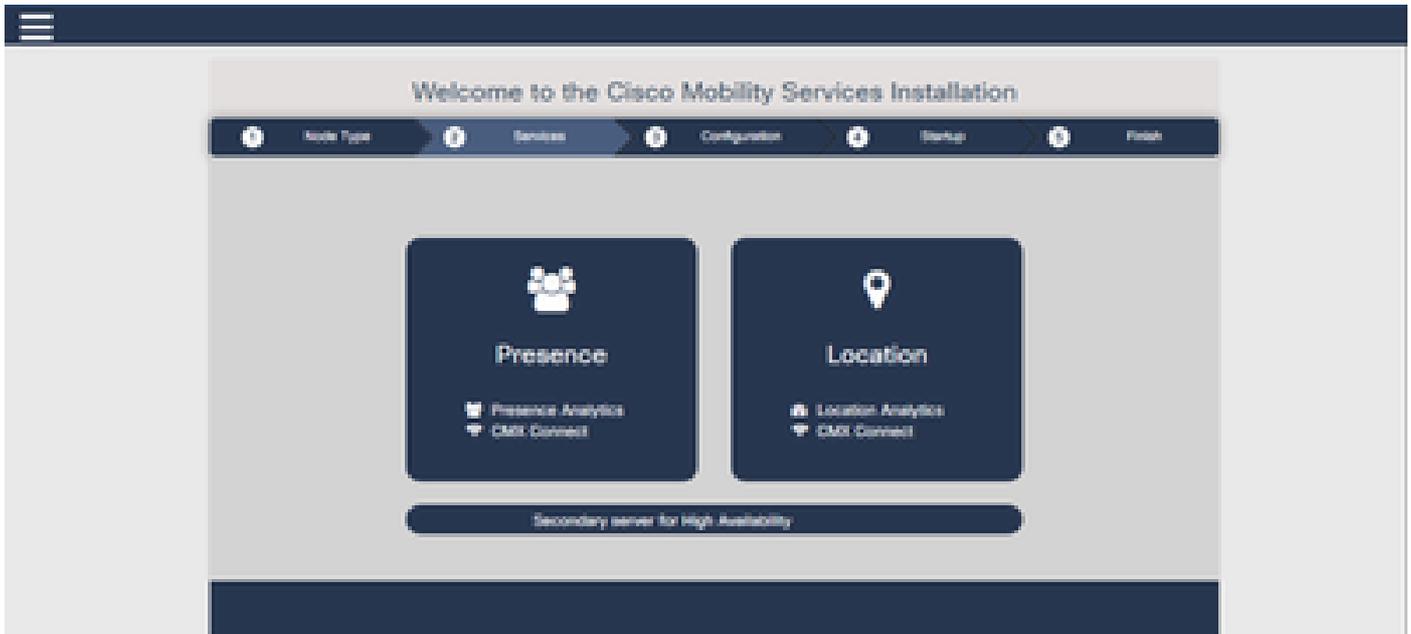
Con il sistema HA installato, dopo un failover gli utenti devono essere reindirizzati alla nuova istanza CMX in esecuzione sul sistema secondario. Per mantenere il failover trasparente dal punto di vista della connettività di rete, verrà utilizzato il concetto di IP virtuale (VIP). Quando nella stessa subnet si trovano sia il server primario che il server secondario, verrà utilizzato un mapping di indirizzi VIP. In questa configurazione, i sistemi esterni sono esposti a un VIP. Questo VIP è mappato all'IP reale del CMX primario in esecuzione. Quando si verifica il failover, viene eseguito un nuovo mapping dell'indirizzo VIP all'indirizzo del CMX secondario. Tutto questo avviene automaticamente senza alcun intervento umano.

L'utilizzo di un IP virtuale non è obbligatorio. Infatti, se si sta eseguendo CMX Layer 3 High Availability (ossia se i due server si trovano in subnet diverse), non è possibile utilizzare un IP virtuale. L'IP virtuale fornisce un IP univoco per l'amministratore IT (o Prime Infrastructure/ Cisco DNA Center) per gestire CMX indipendentemente da failover o failback. I WLC, tuttavia, hanno un tunnel NMSP solo verso l'indirizzo IP fisico CMX attualmente attivo.

## Passaggio 1. Installazione interfaccia Web

Installazione primaria:

Installare CMX normalmente con il login in [https://cmx\\_ip\\_address:1984/](https://cmx_ip_address:1984/). Nel programma di installazione Web, selezionare il tipo di nodo Presenza o Posizione. Per questo tipo di installazione non è necessario specificare il tipo di nodo come primario. Si tratta di un server autonomo che può essere eseguito come server primario, come mostrato nell'immagine.



Installazione secondaria:

Installare CMX ([https://cmx\\_ip\\_address:1984/](https://cmx_ip_address:1984/)) normalmente finché non è necessario selezionare il tipo di nodo nel programma di installazione Web. Una terza opzione è prevista per le licenze secondarie. Se si seleziona questa opzione, il sistema viene configurato come secondario e viene fornito un collegamento all'interfaccia CMX High Availability Admin.

L'interfaccia Web CMX High Availability Admin è in esecuzione sulla porta CMX 4242 ed è accessibile al seguente indirizzo: [https://cmx\\_ip\\_address:4242/](https://cmx_ip_address:4242/). Accedere all'interfaccia Web HA utilizzando l'ID utente cmxadmin e la password configurata per l'ID utente cmxadmin al momento dell'installazione. Dopo aver eseguito l'accesso, l'interfaccia utente dispone di informazioni sullo stato e sulla configurazione. Il ruolo viene visualizzato come secondario per il sistema.



Passaggio 2. Abilita HA

È ora possibile abilitare HA una volta preparati i server principale e secondario. HA può essere attivato nell'interfaccia Web CMX o nella riga di comando CMX. Di seguito sono riportate le opzioni necessarie per impostare HA:

- Indirizzo IP secondario
- Password secondaria: password per l'account cmxadmin sul server secondario
- Indirizzo VIP: indirizzo VIP utilizzato dal server attivo
- Tipo di failover: il failover automatico consente il failover automatico di CMX sul server secondario quando viene rilevato un problema grave. Il failover manuale richiederà all'utente di avviare il failover dall'interfaccia Web o dalla riga di comando. L'errore verrà segnalato all'utente tramite notifiche ma non verrà intrapresa alcuna azione per il failover manuale
- Indirizzo e-mail di notifica: indirizzo e-mail per l'invio di notifiche su problemi o informazioni HA. Le impostazioni e-mail utilizzate per HA sono le stesse di CMX. Questo campo è obbligatorio anche se non si dispone di un server e-mail configurato. Immetti un indirizzo email fittizio e fai clic su "abilita" se non intendi utilizzare le notifiche email.

Configurare il Web HA:

In CMX, passare alla scheda Sistema e fare clic sull'icona Impostazioni. Verrà visualizzata una finestra di dialogo modale con diverse impostazioni in CMX. Selezionare l'opzione HA per visualizzare le opzioni necessarie per abilitare HA. Indirizzo di posta elettronica di notifica è possibile specificare dove si desidera ricevere le notifiche.

Fare clic sul pulsante Abilita quando sono disponibili tutte le opzioni per avviare l'abilitazione di HA.

SETTINGS

- General
- Node Details
- Tracking
- Filtering
- Location Setup
- Mail Server
- Controllers and Maps Setup
- Upgrade
- High Availability**

### High Availability Settings

Secondary IP Address

Secondary Password

Virtual IP Address

Fallover Type

Notification Email Address

CMX verificherà le impostazioni HA e avvierà l'abilitazione di HA tra primario e secondario. WebUI restituirà una volta avviata la configurazione.

Verificare che le impostazioni siano corrette e che la sincronizzazione sia in corso verificando la presenza di una tabella "Alta disponibilità" nella pagina delle impostazioni di CMX. Se tale tabella non è presente e, quando si torna alla sezione delle impostazioni HA, tutti i campi di configurazione sono vuoti, le informazioni sono errate o errate.

SETTINGS

Tracking

Filtering

Location Setup

Mail Server

> Controllers and Maps Setup

Upgrade

High Availability

## High Availability Settings

Help

High availability is enabled and will continue to synchronize data in the background. Synchronization will take time and is completed when the high availability state changes to *Primary Active*. To follow the progress of the sync, please go to 10.0.20.3:4242 for primary and 10.0.20.3:4242 for secondary.

Secondary IP Address

10.0.20.3

Secondary Password (Please use the password for the CLI user cmxadmin)

\_\_\_\_\_

Use Virtual IP Address

Virtual IP Address

10.0.20.10

Failover Type

Auto

Notification Email Address (Please use a space, comma, or semicolon to separate each email address)

\_\_\_\_\_

Disable

Close Save

L'abilitazione di HA non è stata tuttavia completata. La sincronizzazione iniziale di tutti i dati tra il server principale e quello secondario può richiedere molto tempo. L'interfaccia utente indicherà lo stato come Sincronizzazione primaria durante l'esecuzione della sincronizzazione.

Al termine della sincronizzazione, il server sul server primario passerà allo stato Primary Active (Primario attivo).

Una volta completato, verrà generato un avviso relativo alle informazioni in CMX. Inoltre, verrà inviato un avviso tramite e-mail che indica che il sistema è attivo e in fase di sincronizzazione.

Abilitare High Availability CLI (per riferimento):

```
cmxadmin@localhost:~$
login as: cmxadmin
cmxadmin@10.0.20.2's password:
Last login: Tue May 22 16:03:42 2018
cmxadmin@localhost ~]$ cmxha config
Usage: __main__.py config [OPTIONS] COMMAND [ARGS]...

Configure CMX high availability configuration

Options:
  --help  Show this message and exit.

Commands:
  disable  Disable CMX high availability configuration
  enable   Enable CMX high availability configuration
  modify   Modify CMX high availability configuration
  test     Test CMX high availability configuration
cmxadmin@localhost ~]$ cmxha config enable
Are you sure you wish to enable high availability? [y/N]: y
Please enter secondary IP address: 10.0.20.3
Please enter the cmxadmin user password for secondary:
Do you wish to use a virtual IP address? [y/N]: y
Please enter the virtual IP address: 10.0.20.10
Please enter failover type [manual|automatic]: automatic
Please enter an email address(es) for notifications (Use space, comma or semicolon to separate): jidalal@cisco.com
```

## Passaggio 3. Aggiungi Cisco WLC a CMX

È possibile aggiungere i WLC Cisco usando la CLI o l'interfaccia utente CMX, o usando Prime Infrastructure. Per questa esercitazione, è possibile aggiungere elementi direttamente utilizzando CMX WebUI.

La configurazione del controller funziona solo se la connessione NMSP è corretta. Tuttavia, anche se il controller può essere aggiunto correttamente, ma la connessione potrebbe non funzionare.

Passare al server CMX primario [https://cmx\\_ip\\_address/](https://cmx_ip_address/). Fare clic sulla scheda Sistema > Icona Impostazioni > Menu a sinistra.

SETTINGS
✕

- Tracking
- Filtering
- Location Setup
- Mail Server
- ▼ Controllers and Maps Setup
- Import
- Advanced

## Maps

Please select maps to add or modify:

Browse...

Delete & replace existing maps & analytics data

Delete & replace existing zones

Upload

---

## Controllers

Please add controllers by providing the information below:

<b>Controller Type</b>	<input style="width: 90%; border: 1px solid #ccc;" type="text" value="WLC"/>
<b>IP Address</b>	<input style="width: 90%; border: 1px solid #ccc;" type="text" value="10.0.20.100"/>
<b>Controller Version [Optional]</b>	<input style="width: 90%; border: 1px solid #ccc;" type="text" value="8.3.140"/>
<b>Controller SNMP Version</b>	<input style="width: 90%; border: 1px solid #ccc;" type="text" value="v2c"/>
<b>Controller SNMP Write Community</b>	<input style="width: 90%; border: 1px solid #ccc;" type="text" value="cm"/>

Add Controller

Close
Save

Dopo aver aggiunto i WLC Cisco, è necessario verificare se lo stato del controller è attivo e in esecuzione.

Per convalidare lo stato del controller con l'uso dell'interfaccia utente, è necessario selezionare la scheda Sistema. L'elenco dei controller viene visualizzato nella scheda e il nuovo controller deve essere visualizzato in verde.

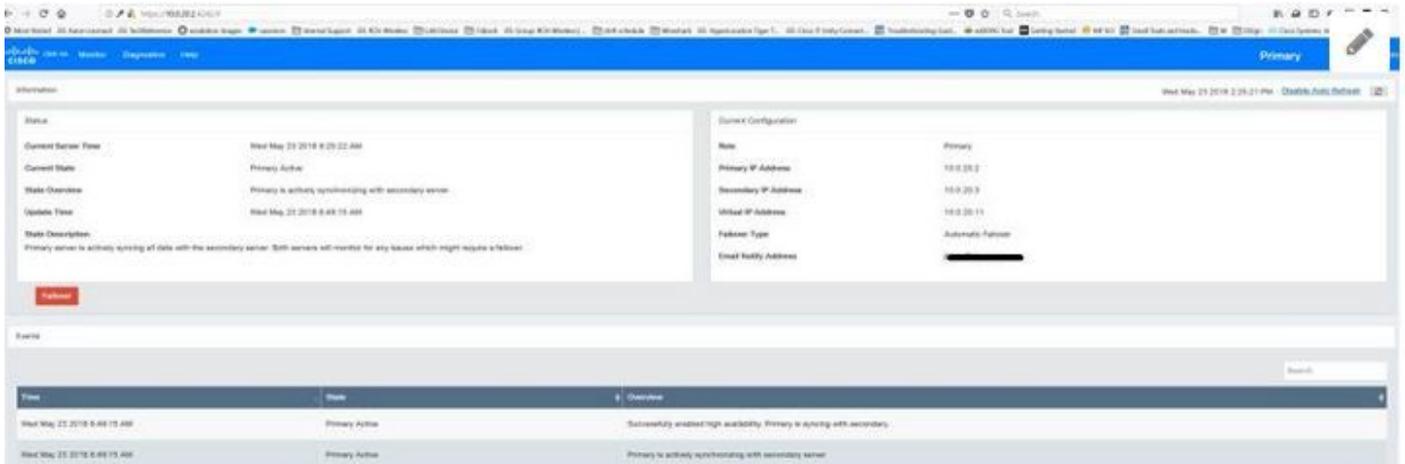
## Passaggio 4. Failover

Il processo di failover comporta il trasferimento delle operazioni al CMX secondario in caso di inattività del sistema principale. Il failover può avvenire automaticamente quando CMX rileva un problema con il server principale. Il failover può essere eseguito manualmente da un utente tramite l'interfaccia utente Web o la riga di comando. L'avanzamento del failover può essere monitorato in base allo stato corrente di ciascun sistema.

Il processo di failover può essere avviato manualmente dall'utente. Il failover può essere eseguito tramite l'interfaccia Web CMX High Availability o la riga di comando CMX.

Failover manuale Web:

Accedere all'interfaccia Web CMX HA sul sito principale o secondario (<https://server ip:4242>). La pagina di monitoraggio contiene un pulsante denominato Failover se i server stanno eseguendo attivamente la sincronizzazione. In alto a destra abilitare l'aggiornamento automatico.



CLI failover manuale (per riferimento):

```
[cmxadmin@localhost ~]$ cmxha failover
Are you sure you wish to failover to the secondary? [y/N]: y
Starting failover from primary to secondary server: 10.0.20.3
Syncing primary files to secondary
Configuring secondary server for Failover
Configuring primary server for Failover
Failover to secondary server has completed successfully
[cmxadmin@localhost ~]$
```

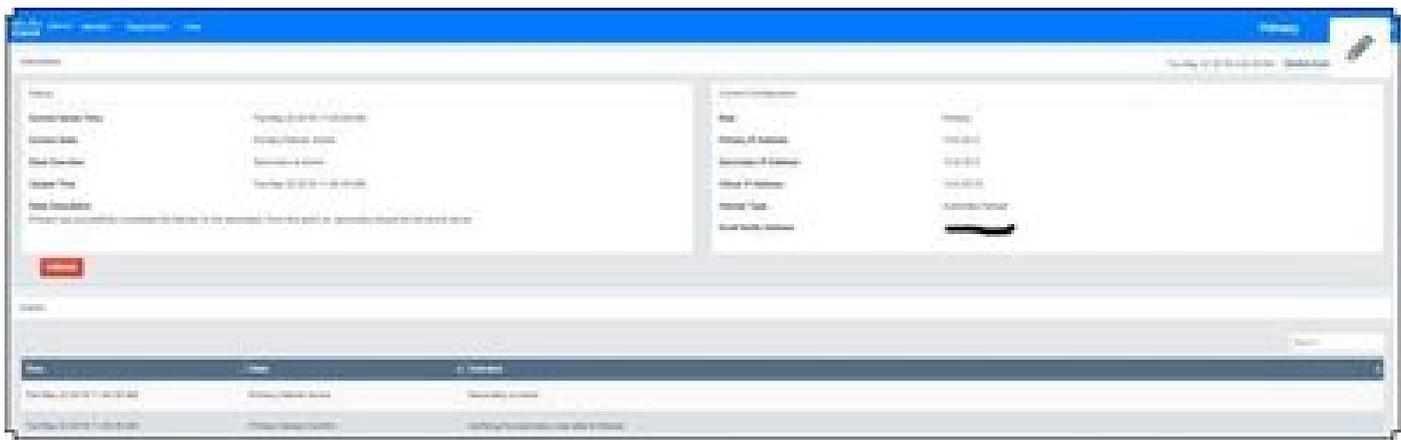
## Passaggio 5. Failback

L'esecuzione di CMX sul database secondario deve essere considerata una situazione temporanea finché non viene identificata la causa principale dell'errore primario. Una volta ripristinata la casella principale (o fornita una nuova casella), è necessario avviare il processo di failback. L'altra opzione consiste nel convertire il sistema in un server primario e sostituire o convertire l'altro sistema in un server secondario. In entrambi i casi, un server deve essere reso disponibile il prima possibile, poiché HA non è più sincronizzato con un server secondario.

Il processo di failback deve essere eseguito manualmente dall'utente. Il failback può essere eseguito tramite l'interfaccia Web CMX HA o la riga di comando CMX.

Failback manuale Web:

Accedere all'interfaccia Web CMX HA sul sito principale o secondario (<https://server ip:4242>). Se entrambi i server indicano che è attivo un failover, nella pagina del monitor sarà presente un pulsante con l'etichetta Failback.



Interfaccia grafica di failback manuale:

```

cmxadmin@localhost ~]$ cmxha failback
Are you sure you wish to failback to the primary? [y/N]: y
Starting to failback to primary server from secondary server 10.0.20.1
Starting to synchronize data from secondary to primary server
.....
Completed synchronization of data from secondary to primary server
Starting to synchronize data from primary to secondary server
.....
Completed failback to primary server
cmxadmin@localhost ~]$

```

## Passaggio 6. Aggiorna/Disabilita HA

Nel formato corrente di CMX è necessario disattivare HA per eseguire un aggiornamento. Per disabilitare HA dalla riga di comando, eseguire `cmxha config disable` dal CMX primario

```

login as: cmxadmin
cmxadmin@10.0.20.3's password:
Last login: Tue Jun  5 15:15:55 2018
[cmxadmin@localhost ~]$ cmxha config disable
Are you sure you wish to disable high availability? [y/N]: y
Do you wish to disable high availability only on the current server? [y/N]: y

```

Se si dimentica di interrompere HA prima di un aggiornamento, lo script di aggiornamento lo ricorda. Prima di riformare HA, sarà necessario aggiornare separatamente il server CMX secondario.

## Come ricaricare in modo sicuro una coppia CMX HA

Eseguire i passaggi successivi per ricaricare la coppia CMX HA:

- Spegnere CMX secondario
- Riavvia CMX primario
- Verificare che il CMX primario sia attivo e in esecuzione
- Accendere il CMX secondario
- Verifica stato HA: `cmxha info`

## Verifica

Attualmente non è disponibile una procedura di verifica per questa configurazione.

## Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

HA dispone della Guida in linea per la funzione. La Guida è completa per e fornisce una panoramica e ulteriori dettagli su questa funzione. È possibile accedervi al seguente indirizzo:

[https://cmx\\_ip\\_address:4242/help](https://cmx_ip_address:4242/help)

Guida di riferimento ai comandi per CMX HA:

[https://www.cisco.com/c/en/us/td/docs/wireless/mse/10-3/cmx\\_command/cmxcli103/cmxcli10-3\\_chapter\\_010.pdf](https://www.cisco.com/c/en/us/td/docs/wireless/mse/10-3/cmx_command/cmxcli103/cmxcli10-3_chapter_010.pdf)

Pacchetto di file da controllare dal registro TAR:

- cmx-hafile-sync
- cmx-haweb-service
- cmx-haserver

## Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).